

Shutdown and Isolate Systems

ICS4ICS Procedure Template

|  |
| --- |
| Instructions The following are suggestions about how you can complete this template that is designed to quickly decide and execute system shutdown or isolation as needed to protect other systems on the network:   * Identify the roles required on the Decision Team that will manage Shutdown and Network Isolation decisions * Review and update the Decision Considerations based on your company requirements * Develop the technical procedures and tools (e.g., script, automation, etc.) to expedite system shutdown and network isolation * Test this Shutdown/Isolation Procedure and update as appropriate |
| DisclaimerISA, ISAGCA, and the ICS4ICS Program provide this template to help asset owners create procedures to perform ICS4ICS and/or Cyber Incident Response and/or other related tasks. Each Asset Owners must update this template based on the needs of their company and ensure the procedure is review and approved by the appropriate parties (e.g., legal, senior management, corporate governance, government relations, etc.) from within their company. |

## Purpose

This document is intended to provide information to help your company quickly make and execute decisions about shutting down or isolating systems that potentially could impact other systems on the company network.

## Situation Trigger

Malware has been detected or a ransomware demand has been made requesting payment to unlock systems AND other systems appear to be at risk of being infected by the same malware.

## Symptoms

OT and/or IT systems are currently being impacted by malware, and normal procedures have not worked to remove the malware or recover the impacted OT and/or IT Systems and the recovery appears lengthy or not possible.

## Escalation

Normal escalation procedures must be used which results in notification to an authorized Incident Commander, if the malware cannot be removed or isolated.

## Declaration

The Incident Commander will declare an Incident, if appropriate

## Decision Timing

The decision to disconnect systems and/or shut them down must be made and executed immediately after identifying that malware has infected systems.

## Decision Needed before Decision Team is formed

The decision to disconnect systems and/or shut them down may have to be made before the Decision Team can be formed. This decision would be based on an immediate threat to other systems and other company operations. This type of decision would likely only be required during weekends and hours when management is not onsite. The company must determine who is authorized to make these decisions during off days/hours which may include:

* Incident Commander (if they can be reached to make the decision)
* Other senior managers (if they can be reached to make the decision)
* The most senior manager who is onsite during off days/hours (7X24)
* Other staff onsite during off days/hours (7X24)

## Decision Team

The following parties will be engaged to assess the situation, make decisions, and determine next steps:

* Incident Commander (DECISION APPROVER/FACILITATOR – or add the approver to the team)
* Operations Section Chief
* Stakeholders in other assets / systems that may be impacted
* Intelligence Analyst (part of Operations Section) – if available
* ICS Cybersecurity Expert (or mutual aid partner) – if available

## Operations Section (Cyber Incident Response Team) INPUTS

The Decision Team will consider the following information provided by the Operations Section Chief, that comes from the Cyber Incident Response staff, when making decisions:

* Information about the malware from public sources
  + DHS CISA and other government agencies around the world provide information about current product vulnerabilities and other risks that may impact numerous asset owners
  + Vendors will provide information about product vulnerabilities which may include fixes and other solutions to manage these vulnerabilities
* Information about the malware from paid sources including mutual aid providers (e.g., Dragos, Mandiant, consultants) – if appropriate
  + Several companies provide information about vulnerabilities for a fee
  + Some companies provide monitoring services to help identify threats to asset owner systems
* Likelihood that malware will spread to other systems (e.g., similar systems components to those that are infected)
  + The company inventory can be used to identify other systems and components that may be at risk; Systems and components by the same OT manufacturers running the same versions of software and/or firmware may be a greater risk

## Decision Criteria

The Decision Team will use these criteria to make decisions about system shutdown and/or isolation:

* Safety and environmental threats and risks
  + The Safety Officer should be able to provide this information
* Operations Section (Cyber Incident Response Team) INPUTS above
* Ability of systems to continue to operate while disconnected from the company network
  + The OT Team should be able to provide this information
* Financial and other business impacts to the company of shutting down/isolating each system
  + Business representatives should be able to provide this information
* Other criteria the company defines

NOTE: The criteria for making Shutdown/Isolation Decisions must be very clear, particularly if others will be making the decision during off days/hours when the Decision Team is not available. A documented decision tree can be very helpful to ensure timely and consistent decisions. Terms and language must be defined to ensure Decision Team members and staff who provide input understand each other.

## Shutdown/Isolation Decision and Execution

These steps will be taken to Shut down or Isolation systems from the network:

* Engage authority to execute the Shutdown/Isolation approval processes
  + This procedure will document who must approve these decisions and ensure they have sufficient Delegation of Authority; For example, the Incident Commander engages the Crisis Management Team to obtain approval
* Use Communication Protocol to inform the appropriate people of the decision (e.g., Disconnect other systems from the enterprise network and/or shutdown systems)
  + This procedure will document the Communication Protocol including who must be informed of the decision)
* The Decision Team will instruct the appropriate staff to Shut down or Isolation systems from the network
  + ICS staff will develop procedures to shut down their systems when this procedure is developed and identify primary, secondary, and tertiary staff who can execute the procedures
  + Network staff will develop scripts to update the Network Firewalls to Isolate Systems and identify primary, secondary, and tertiary staff who can execute the procedures
    - Scripts will be developed to expedite the execution of these procedures